FINAL

NASA APPROACH TO SPACECRAFT/instrument PRODUCT ASSURANCE

— TYPICAL JPL PROGRAM —

Tom E. Gindorf

4/26/95

PRODUCTASSURANCE ELEMENTS

- Quality Assurance
- Electronic Parts Reliability Engineering
  - Environmental Requirements
  - Reliability
- Software Product Assurance
- System Safety

PRODUCT ASSURANCE = "VALUE ADDED"

Product Assurance Discipline	Examples of Value Added
Electronic Parts Reliability Engineering	• Assist in obtaining highest quality parts appropriate to mission and to project resource constraints • Thoroughly analyze parts failures • Provide consultation to electronic equipment designers • Reduce costs through common buys • Avoid problems through parts-alerts monitoring
Environment Requirements	• Provide technical criteria for design of flight equipment to operate within ground operations and mission environments • Define and oversee implementation of efficient productive environmental testing

PRODUCT ASSURANCE = "VALUE ADDED" (cont.)

Product Assurance Discipline	Examples of Value Added
Quality Assurance	• Process evaluation and problem resolution • Failure-prevention controls development • Advanced interconnect development/qualification • Hardware-manufacturing/training • Inspection and documentation to assure quality workmanship
Reliability	• Provide electronic and mechanical hardware-reliability design support throughout development cycle • Validate PFR closure for adequate resolution and verification of corrective action

PRODUCT ASSURANCE = "VALUE ADDED" (cont.)

Product Assurance Discipline	Examples of Value Added
Software Product Assurance	• Support the development of software requirements, design, coding, inspection cycles — early problems/defect avoidance and detection reduces software development costs
System Safety	• Provide engineering support to hardware and software design to ensure they function without a safety-related anomaly
	• Provide safety engineering support to ensure compliance with launch-agency requirements
	• Ensure safety in flight hardware ground handling (for both hardware and personnel)

PROJECT/PRODUCT ASSURANCE LIFECYCLE PHASES AND EVENTS

QA - **QUALITY** ASSURANCE

SAFETY = SYSTEMS SAFETY

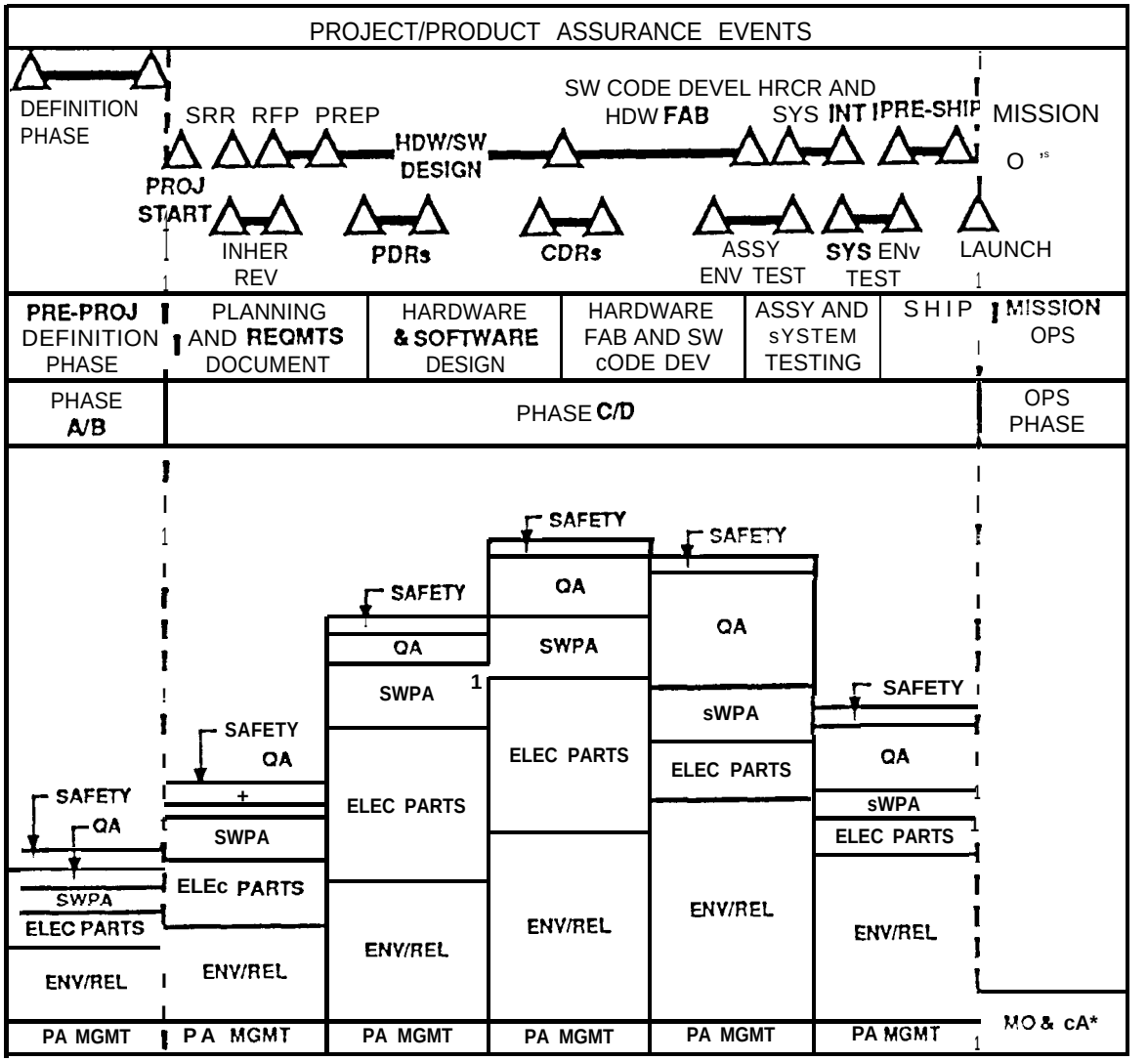
SWPA = SOFTWARE PRODUCT ASSURANCE

ELEC PARTS = **ELECTRONIC** PARTS RELIABILITY

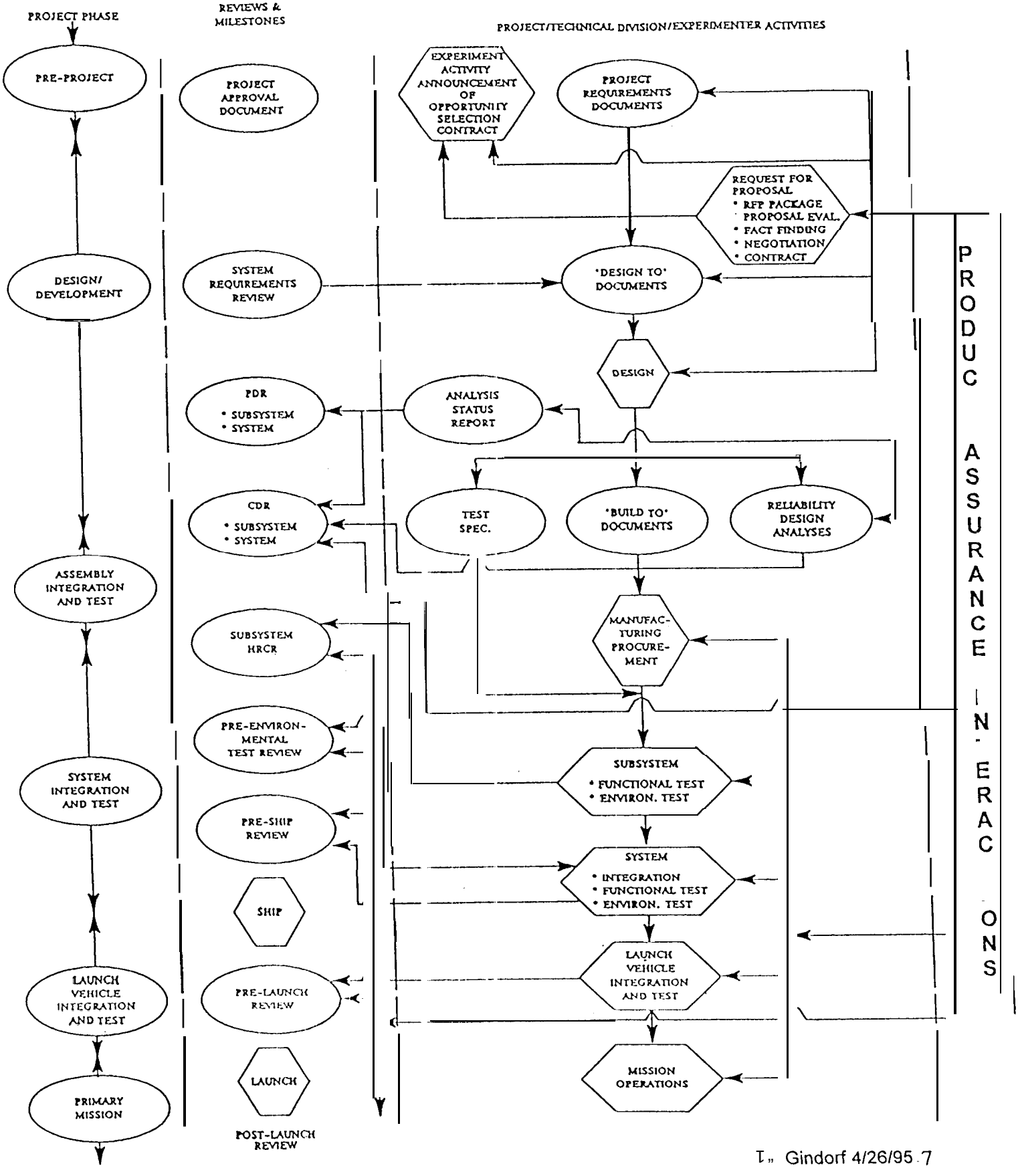
ENV/REL = ENVIRONMENTAL REQUIREMENTS & RELIABILITY

PA MGMT = PRODUCT ASSURANCE MANAGER

- MO&CA= MISSION Operations AND COMMAND ASSURANCE



FLOW OF PRODUCT ASSURANCE INTO PROJECT EVENTS



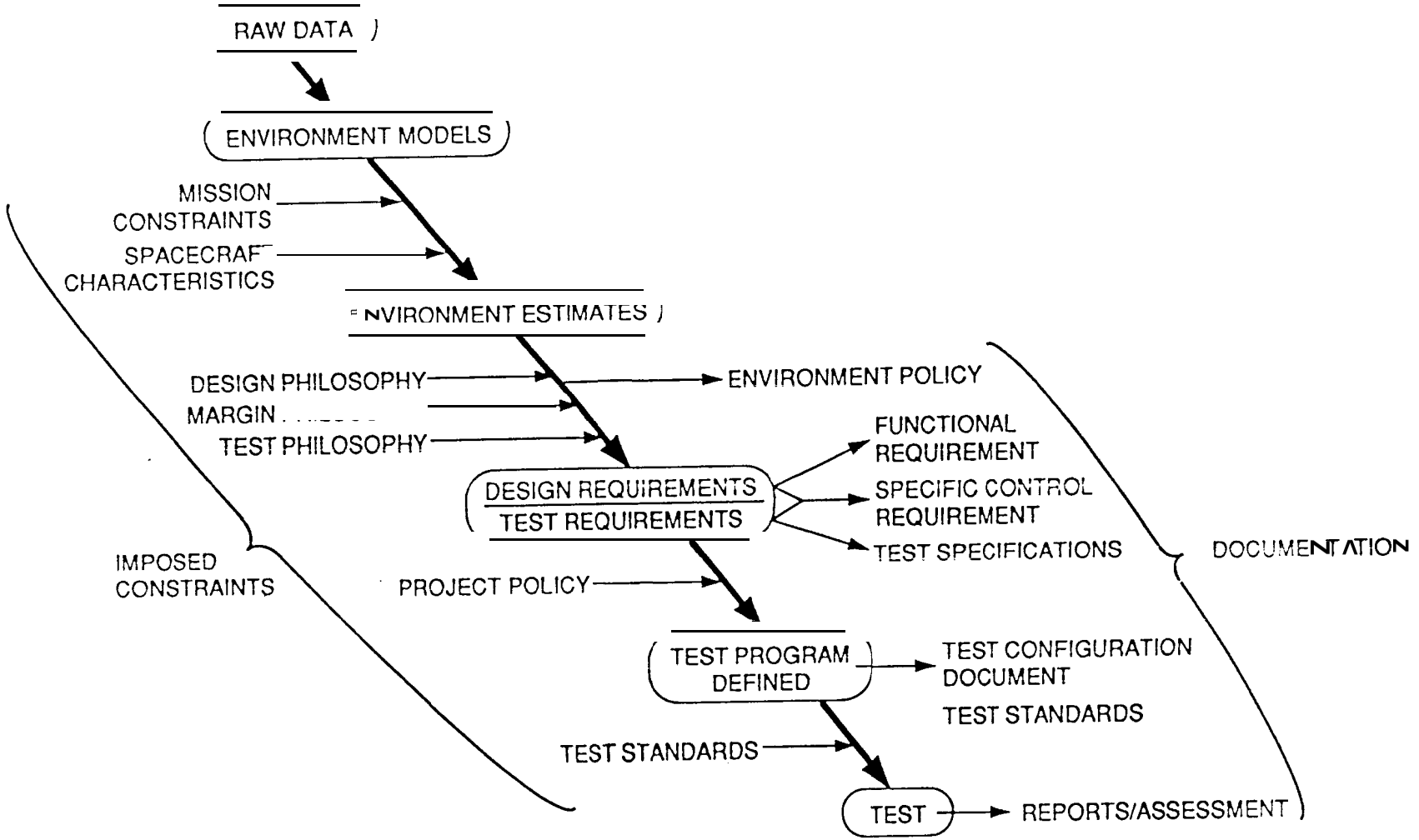
QUALITY ASSURANCE FUNCTION

- Planning of project and contractor QA hardware effort
- Independent information source for quality, status and assessment of hardware
- Contribution to hardware development
  - Ensure hardware conforms to requirements (monitor contractors)
  - Inspect./observe hardware fabrication
  - Detect problems early
  - Implement corrective action
  - Verify test performance to specification/procedures
  - Train and certify (soldering, polymeric, etc.)
  - Evaluate qualification status of fabrication and rework processes
- Review/approval of manufacturing plans, procedures, and subcontractor QA documents
- Inspection and observation
  - Handling and transportation packaging
  - Hardware integration (receiving inspection, data packaging review, bonded stores)

ENVIRONMENTAL REQUIREMENTS FUNCTIONS

- Systematic and structured design and test requirements that, upon implementation, demonstrate confidence in mission environmental compatibility
- Visible management structure for consistent implementation of the environmental programs and individual projects across the Laboratory
- Evaluations and assessments of hardware environmental risks

ENVIRONMENTAL PROGRAM INFORMATION FLOW



ENVIRONMENTAL PROGRAM RESPONSIBILITY/AUTHORITY SUMMARY

		Developed By	Authorized By
REQMTS	General environmental policy/requirements	Reliability Engineering	Project/task or space-craft system manager
IMPLEMENT	Detail environmental test requirements	Cognizant engineer	Environmental/ reliability engineer
	Test procedures	Test agency	Cognizant engineer
	Test performance	Test agency	Cognizant engineer
EVAL	Test reporting	Cognizant engineer and test agency	Environmental/ reliability engineer determines pass/fail

RELIABILITY ENGINEERING

RELIABILITY FUNCTIONS

- Planning (RFPs, Requirements)
- Controls (ECRs, PFRs, Waivers, DDRs, Status Reports
- Analysis
  - Electronic circuit stress analysis and review
  - Worst-case analysis and review
  - Radiation circuits effects analysis and review
  - ECRS analysis/approval
  - Waivers analysis/approval
  - PFRs analysis/approval
  - Thermal stress to piece part level (T_J rise)
  - Failure analysis and reporting
  - Fault tree analysis (FTA)
  - Failure mode effects criticality analysis (FMECA)
  - Mathematical modeling
  - Numerical reliability prediction for trade studies
  - Maintainability
  - Availability
- Technical Reviews and Risk Assessments

RELIABILITY ENGINEERING

PROBLEM/FAILURE REPORTING

JPL
Jet Propulsion Laboratory
California Institute of Technology
4800 Oak Grove Drive
Pasadena, California 91109

PROBLEM/FAILURE REPORT

No. 54185

1. PROJECT: GALILEO
2. WRITTEN BY: JPL
3. PROBLEM/FAILURE DATE: 12/13/88
SAF QA # 1369
6. SUBSYSTEM: 2010
NOMENCLATURE: RPM
11. REPORTING LOCATION: JPL SEC. 353 — OTHER: IN TRANSIT
12. PROBLEM/FAILURE NOTED DURING: OTHER: Transportation
13. SPECIFIC ENVIRONMENT: OTHER: Packing Case
14. DESCRIPTION OF PROBLEM/FAILURE – RPM TRANSPORTATION SHOCK –

During the transportation of the RPM from MBB, West Germany, to JPL, the RPM packing case experienced a shock which resulted in damage to the temperature/humidity recording instrument, and the subsequent loss of future humidity recording. Preliminary review of the three Axis Accelerometer Recorders indicates low level shock was imparted to the RPM support structure within the packing case. This document is to assure that the shock recorder's data are reviewed by MBB personnel and that an analysis and report (CONTINUED ON PAGE 2)

ORIGINATOR: Carl S. Engelbrecht — DATE: 1/5/89 — COGNIZANT ENGINEER: Jack O. Patzold

I ORIGINATOR

15. VERIFICATION AND ANALYSIS

The shock recorder strip chart was analized by the shock recorder manufacturer (see pages 3 and 4 of the attached NCR RPM-NC 885), and the shock level sustained by the RPM was confirmed to be within admissable limits (Ref. RPM-NC 885). The temperature/humidity recording instrument was damaged because it was not on the damped portion of the RPM transporter, and because it is made for stationary use only. Though the humidity was not measured after the shock, it could not have exceeded 65% because the desiccants within the container remained blue (Ref. RPM-NC 885 and desiccant spec.). NOTE: The humidity of the RPM environment is not critical (the RPM is frequently stored in non-environmentally controlled areas).

16. CAUSE OF PROBLEM/FAILURE: DAMAGE (MISHANDLING) — H-2

PERSON COMPLETING SECTION II — DATE: 5-12-89

II VERIFICATION

18. CORRECTIVE ACTION TAKEN

Because the shock level and humidity of the RPM during transportation were within acceptable limits at all times, there is no corrective action required. The action required in section 14 above (i.e. a review of the shock recorder data and an analysis of the situation were completed, and report was submitted by MBB) has been completed by JPL (see attached NCR RPM-NC 885 and attachments) and accepted by JPL (Ref. closure of NCR). The RPM should be used "AS-IS".

19. DISPOSITION OF SUBSYSTEM OR ASSEMBLY: OTHER: use as is
20. EFFECTIVITY: THIS UNIT
22. SIGNATURE COGNIZANT ENGINEER — SEC 353 — DATE 5-12-89 — DATE 6-8-89

III CORRECTIVE ACTION

IV — DATE 6/13/89 — DATE 7/7/89

COPY DISTRIBUTION: WHITE – ACTION COPY, CANARY – PROJECT OFFICE, PINK – PFR CENTER, GOLDENROD – ACCOMPANY HARDWARE

→ EQUIPMENT IDENTIFICATION

→ PROBLEM DESCRIPTION

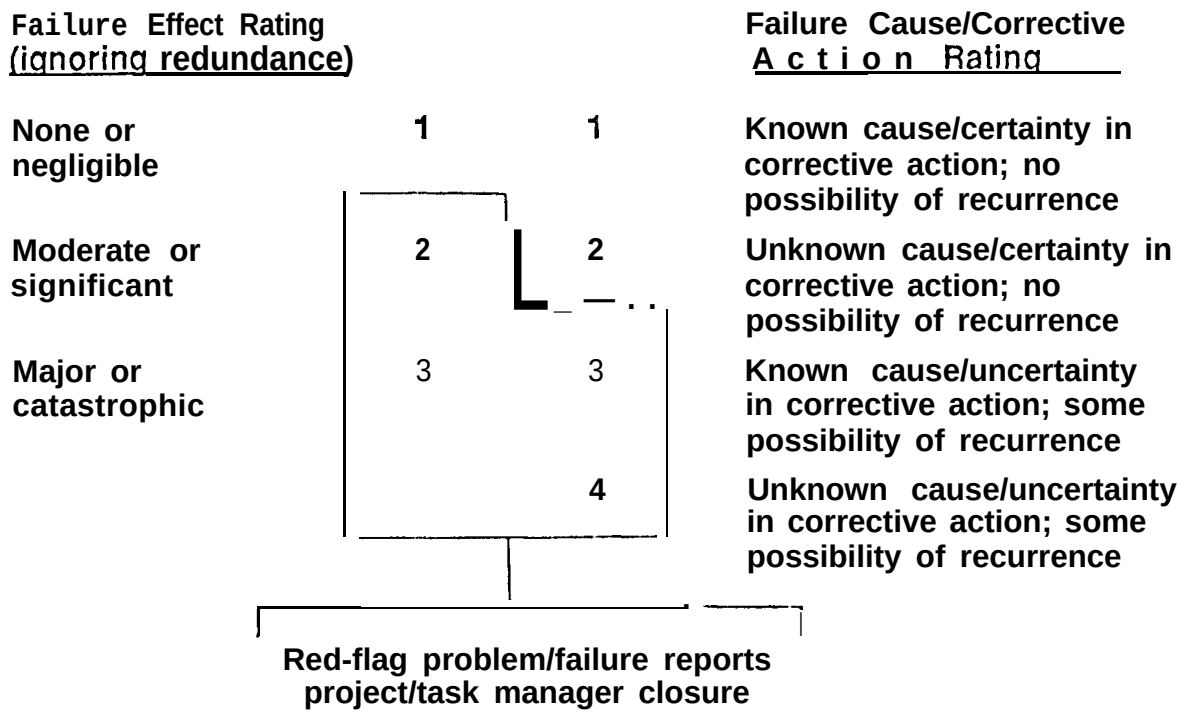
→ PROBLEM ANALYSIS
- MUST ADDRESS THE PROBLEM
- MUST ADDRESS THE EFFECT ON OTHER ITEMS

→ CORRECTIVE ACTION
- MUST ADDRESS THE ANALYSIS AND THE PROBLEM

→ PFR RATING

RELIABILITY ENGINEERING INDEPENDENT REVIEW AND APPROVAL
- CORRECTIVE ACTION IMPLEMENTED
- GATE PASSED WHICH CAUSED THE PROBLEM

PFR RATING CHART



RELIABILITY ENGINEERING

MISSION RISK ASSESSMENT BASED ON PFR RATINGS

	Failure Cause/Corrective Action Rating			
	Certain Corrective Action		Uncertain Corrective Action	
Failure Effect Rating	Known Cause (1)	Unknown Cause (2)	Known Cause (3)	Unknown Cause (4)
None or Negligible (1)	No Additional Mission Risk		Negligible Additional Mission Risk	
Moderate or Significant (2) or Major or Catastrophic (3)			Known or Potential Additional Mission Risk (RED FLAG)	

SOFTWARE PRODUCT ASSURANCE FUNCTION

- Goal
  - To help improve the operation reliability of projects while in flight
    - An effort to detect and correct, as early as possible, errors that exist in the commanding process to eliminate command errors sent to the spacecraft
- To achieve this goal, during mission operations
  - Review flight operations documentation and processes, and recommend modification to improve the process
  - Monitor the command process
  - Monitor the problem/failure reporting system
  - Participate with flight teams in analyzing command incidents and developing corrective actions

SYSTEMS SAFETY FUNCTION

- Develop and implement a project safety plan and schedule (preproject to launch) that will meet all appropriate safety requirements
- Develop a safety-oriented organization to minimize risk to people and hardware, and to maximize probability of project success
- Ensure the priority of project's safety role and that personnel safety is not compromised

SUMMARY

- Many pressures to reduce cost
- Determining the proper balance between cost and risk needs more attention
- Ultimately any failure is viewed as bad regardless of what is agreed upon initially
- Great and interesting challenge for Safety & Mission Assurance to determine what the future product assurance requirements should be